CLAIMS

What is claimed is:

1. A method of enhancing throughput of a pipelined encryption/decryption engine for an encryption/decryption process comprising a predetermined number of stages and providing feedback around the stages, the method comprising the steps of:

receiving a source datablock for a given stage and encryption/decryption context identifier;

indexing according to the encryption/decryption context identifier into a bank of initial variables to retrieve an initial variable for the source datablock, the bank comprising a plurality of initial variables for each encryption/decryption context identifier; and

generating an output datablock from the source datablock and its corresponding initial variable.

2. The method of claim 1 wherein in the indexing step the bank of initial variables comprises a number of initial variables for each encryption/decryption context identifier that is at least as large as the predetermined number of stages.

3. The method of claim 1 additionally comprising the step of replacing the corresponding initial variable with the output datablock.

4. The method of claim 1 wherein the encryption/decryption process comprises Cipher Block Chaining Mode with exception of handling of initial variables.

5. The method of claim 4 wherein the encryption/decryption process comprises a block cipher capable of being pipelined.

6. The method of claim 5 wherein the process is Digital Encryption Standard (DES).

7. A method of enhancing throughput of a pipelined encryption/decryption engine for an encryption/decryption process comprising a predetermined number of stages and providing feedback around the stages, the method comprising the steps of:

for each of a plurality of encryption/decryption contexts, a number of which equals or exceeds the predetermined number of stages, receiving a source datablock for the corresponding encryption context identifier;

for each of the plurality of encryption/decryption contexts, indexing according to the encryption/decryption context identifier into a bank of variables comprising initial variables and prior-stage output datablocks to retrieve a seed variable for the source datablock; and

for each of the plurality of encryption/decryption contexts, generating an output datablock from the source datablock and its corresponding seed variable;

wherein each stage of the pipelined encryption/decryption engine at any given time is processing source datablocks from an encryption/decryption context different than encryption/decryption contexts of source datablocks being processed in all other stages of the pipelined encryption/decryption engine.

8. The method of claim 7 wherein each of the plurality of encryption/decryption contexts comprises a telecommunications data stream to be encrypted.

9. The method of claim 8 additionally comprising the step of decrypting the output datablocks at a plurality of locations distributed from the encryption/decryption engine corresponding in number to the number of encryption/decryption contexts.

10. The method of claim 7 wherein the encryption/decryption process comprises Cipher Block Chaining Mode.

11. The method of claim 10 wherein the encryption/decryption process comprises a block cipher capable of being pipelined such as Digital Encryption Standard (DES).

12. A pipelined encryption/decryption engine for an encryption/decryption process comprising a predetermined number of stages and providing feedback around the stages, the encryption/decryption engine comprising:

means for receiving a source datablock for a given stage and encryption/decryption context identifier;

means for indexing according to the encryption/decryption context identifier into a bank of initial variables to retrieve an initial variable for the source datablock, the bank comprising a plurality of initial variables for each encryption/decryption context identifier; and

means for generating an output datablock from the source datablock and its corresponding initial variable.

13. The encryption/decryption engine of claim 12 wherein in the indexing means the bank of initial variables comprises a number of initial variables for each encryption/decryption context identifier at least as large as the predetermined number of stages.

14. The encryption/decryption engine of claim 12 additionally comprising means for replacing the corresponding initial variable with the output datablock.

15. The encryption/decryption engine of claim 12 wherein the encryption/decryption process comprises Cipher Block Chaining Mode with exception of handling of initial variables.

16. The encryption/decryption engine of claim 15 wherein the encryption/decryption process comprises a block cipher capable of being pipelined such as Digital Encryption Standard (DES).

17. An encryption/decryption engine for enhancing throughput of a pipelined encryption/decryption process comprising a predetermined number of stages and providing feedback around the stages, the method comprising the steps of:

means for, as to each of a plurality of encryption/decryption contexts, a number of which equals or exceeds the predetermined number of stages, receiving a source datablock for the corresponding encryption context identifier;

means for, as to each of the plurality of encryption/decryption contexts, indexing according to the encryption/decryption context identifier into a bank of variables comprising initial variables and prior-stage output datablocks to retrieve a seed variable for the source datablock; and

means for, as to each of the plurality of encryption/decryption contexts, generating an output datablock from the source datablock and its corresponding seed variable;

wherein each stage of the pipelined encryption/decryption engine at any given time is processing source datablocks from an encryption/decryption context different than encryption/decryption contexts of source datablocks being processed in all other stages of the pipelined encryption/decryption engine.

18. The encryption/decryption engine of claim 17 wherein each of the plurality of encryption/decryption contexts comprises a telecommunications data stream to be encrypted.

19. The encryption/decryption engine of claim 18 additionally comprising means for transmitting the output datablocks to be decrypted at a plurality of locations distributed from the encryption/decryption engine corresponding in number to the number of encryption/decryption contexts.

20. The encryption/decryption engine of claim 17 wherein the encryption/decryption process comprises Cipher Block Chaining Mode.

21. The encryption/decryption engine of claim 20 wherein the encryption/decryption process comprisesa block cipher capable of being pipelined such as Digital Encryption Standard (DES).